19 November 2009

Ms. Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

Re: ***Ex Parte* Presentation**
In the Matter of : NBP Public Notice # 8, Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan, Docket No. GN 09-47, et al.

Dear Ms. Dortch:

This is to inform you that Anthony M. Rutkowski, EVP for Regulatory Affairs and Standards of Yaana Technologies LLC, together with Dr. Stephen J. Lukasik, met with the following Public Safety and Homeland Security Bureau staff on 18 Nov 2009 at the Commission's Headquarters:

- Jeffrey Goldthorp, Chief, Communications Systems Analysis Division
- Gregory Cooke, Legal Advisor, Communications Systems Analysis Division
- Richard Hovey, Telecom Specialist, Communications Systems Analysis Division
- Gregory Intoccia, Attorney Advisor, Policy Division

Dr. Lukasik and Mr. Rutkowski are Senior Distinguished Research Fellows at Georgia Tech Center for International Strategy, Technology, and Policy (CISTP). Dr. Lukasik is also well known as former Director of DARPA, former FCC Chief Scientist and Head of the Office of Science and Technology, former Vice President of Xerox, RAND, Northrop and TRW Corporations, and headed the Stanford University Center for International Security and Cooperation programs on infrastructure protection and cybersecurity. Mr. Rutkowski is also the appointed head of the Cybersecurity Rapporteur Group, Q.4/17, International Telecommunication Union Telecommunication Standardization Sector (ITU-T), but not appearing in that capacity.

The purpose of this meeting was to be responsive to the cybersecurity issues posed in NPB Public Notice #8 and provide an overview of current significant initiatives contained in the attached presentation. This material reflects the discussions at this meeting.

Pursuant to the Commission's rules, this *ex parte* letter is being filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceeding.

Respectfully submitted,

/s/

Anthony M. Rutkowski
SVP for Regulatory Affairs and Standards
Yaana Technologies, LLC
500 Yosemite Drive, Suite 120
Milpitas, CA 95035
tel: +1 408.854.8041
mailto:tony@yaanatech.com

attachment: **Toward Global Cybersecurity in the Broadband Infrastructure**

NBP Public Notice # 8
Pleading Cycle

GN Docket No. 09-47

Cybersecurity Comments

FCC
Washington DC
18 Nov 2009

Toward Global Cybersecurity in the Broadband Infrastructure

Anthony M. Rutkowski
EVP for Regulatory Affairs and Standards, Yaana Technologies
tony@yaanatech.com
Senior Research Fellow, Georgia Tech Center for International Strategy, Technology, and Policy (*CISTP*)
Also Chair, International Cybersecurity Group Q.4/17, ITU-T

Yaana Technologies

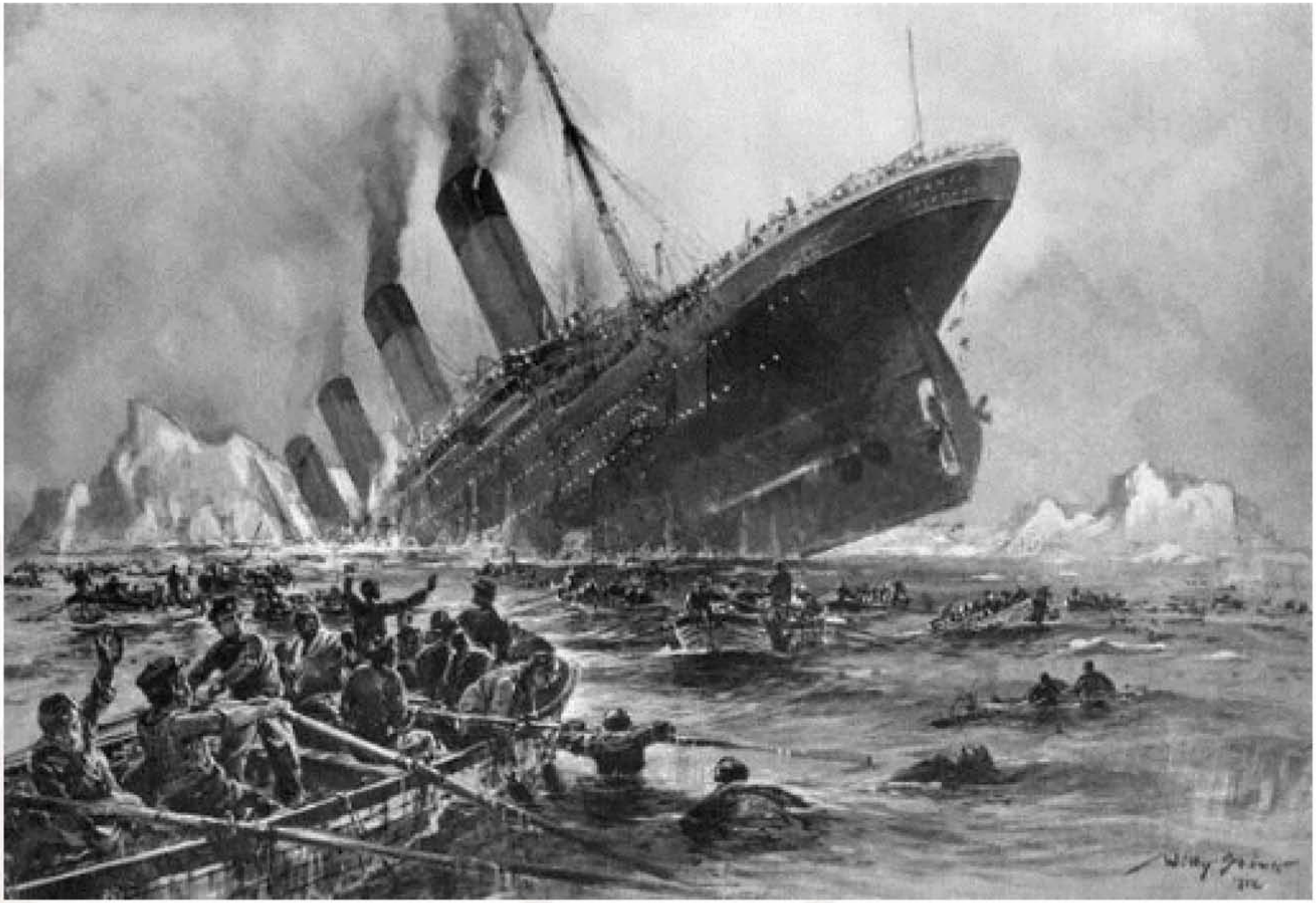
- ❑ Milpitas, California, based company providing
  - – high trust identity management platforms
  - – high trust messaging services
  - – network cybersecurity and forensics compliance capabilities
- ❑ Trusted Third Party operations centers
- ❑ Private sector and government customers
- ❑ Supports domestic U.S. and global cyber security technical activities

The Approaching Cyber Tsunami

- ❑ Network infrastructure/service providers and users are facing extraordinary levels of intentional and unintentional threats
  - – As of July 2009, Spain's Panda Networks was detecting 37 thousand new viruses, worms, Trojans, and other security threats per day
  - – The totals have reached 30 million different varieties and are rapidly evolving
- ❑ The threats are growing exponentially
- ❑ The situation will get worse unless collective global action occurs on implementing infrastructure-based cyber security capabilities

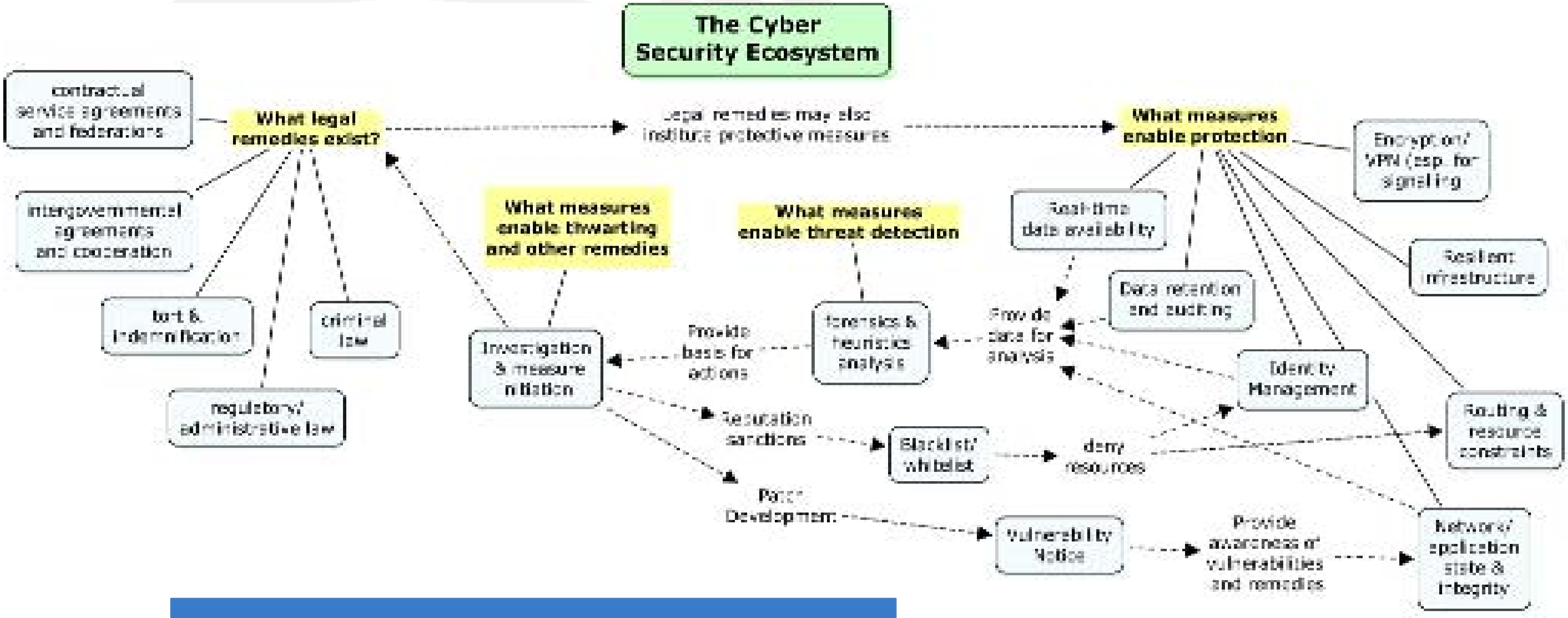
Cyber Tsunami Experiences

- Similar kinds of cyber security challenges were faced a hundred years ago
  - Fast-paced new network technology emerged
  - Networks became global in scope
  - Harmful incidents were rapidly scaling
  - Government policy was not to intervene to avoid harm to innovation
  - Sinking of the Titanic in 1912 finally motivated U.S. government action
- Every new network technology has faced similar challenges
  - The 1980s OSI Internet had public infrastructure security solutions, but lacked innovation
  - The 1990s NSF Internet had no public infrastructure security solutions, but was great for innovation
    - Criminals, hackers, terrorists, miscreants are also innovative with this infrastructure
  - Like the economic system, the wrong balance was struck allowing the NSF Internet to become a public infrastructure free from government oversight
- Solutions have been similar over the past 100 years
  - Obtain global agreement and ongoing cooperation to avoid network harm
  - Strengthen trust and identity management/attribution – especially for providers and network identifiers
  - Compartmentalize network infrastructures
  - Require provider and vendor compliance with security capabilities
  - Establish provider and national monitoring centers with packet inspection and enforcement capabilities



How many cyber icebergs do you need before everyone realizes there is a problem?

What must be done?



The Cyber Security Ecosystem

What legal remedies exist?

contractual service agreements and federations

intergovernmental agreements and cooperation

tort & indemnification

criminal law

regulatory/ administrative law

Legal remedies may also institute protective measures

What measures enable protection

Encryption/ VPN (esp. for signaling)

Real-time data availability

Resilient infrastructure

Data retention and auditing

Identity Management

Routing & resource constraints

Network/ application state & integrity

What measures enable thwarting and other remedies

What measures enable threat detection

Investigation & measure initiation

Provide basis for actions

forensics & heuristics analysis

Provide data for analysis

Reputation sanctions

Blacklist/ whitelist

deny resources

Patch Development

Vulnerability Notice

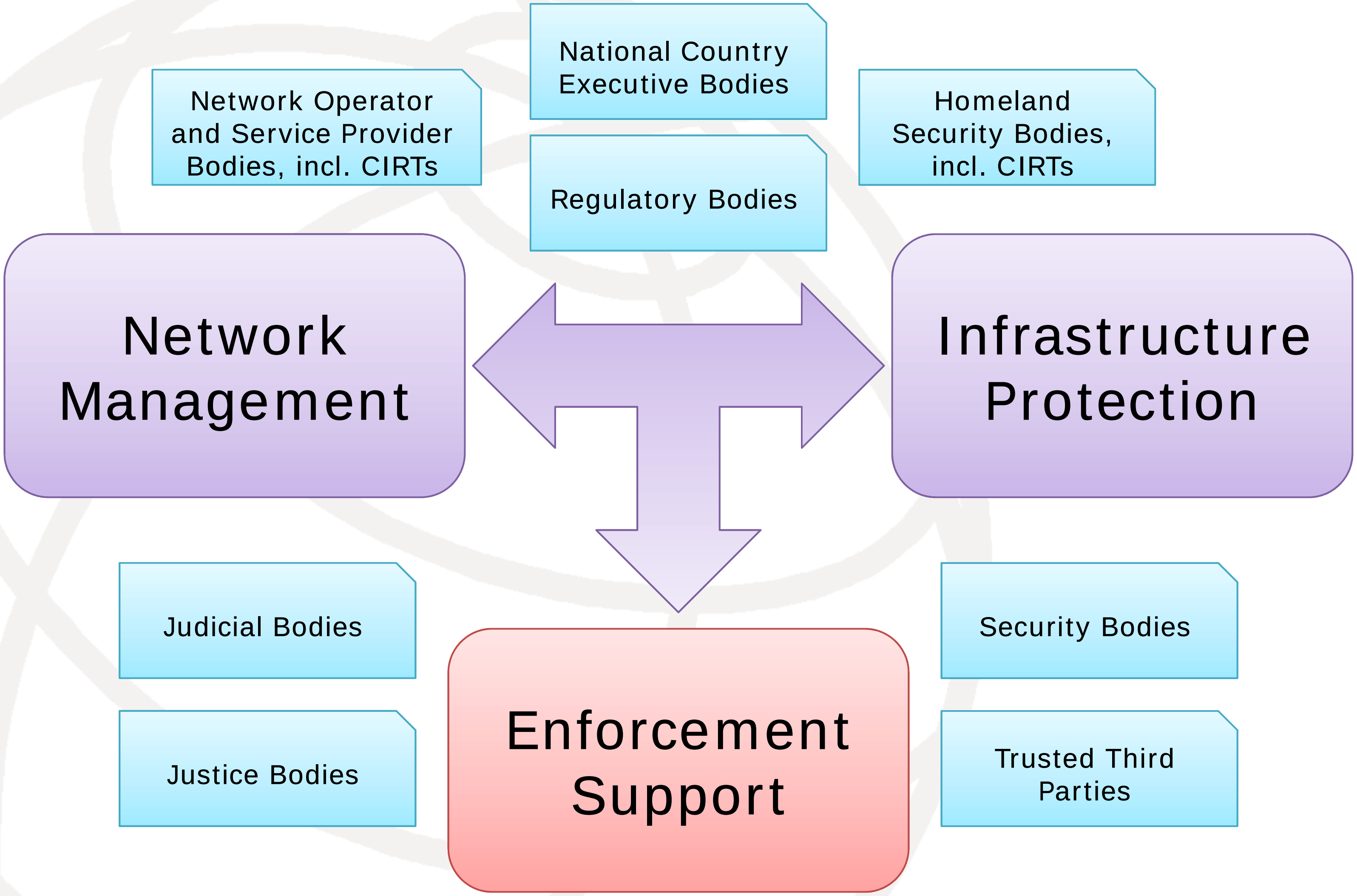
Provide awareness of vulnerabilities and remedies

The needed capabilities are well known

Who can lead / act?

- Government must act
  - Necessary steps are not achievable through industry initiative or the marketplace
  - Scale and complexity too great
  - Incentives do not exist
- Competence largely resides in the NSA and counterparts worldwide
  - Knowledge, expertise, research, leadership
- Jurisdiction resides in national regulatory authorities
  - FCC has sufficient jurisdiction and authority under the Communications Act, CALEA, etc
  - Infrastructure based capabilities can be implemented using a “CALEA model” which exists worldwide
    - The Commission
      - Mandates capabilities based on NSA requirements coordinated with DHS and other relevant agencies
      - Indemnifies compliant providers and vendors
      - Implements strong identity management for providers and network identifiers
    - Industry
      - Develops and implements standards based solutions
      - Performs compliance testing

Current Cyber Convergence



National Country Executive Bodies

Network Operator and Service Provider Bodies, incl. CIRTs

Regulatory Bodies

Homeland Security Bodies, incl. CIRTs

Network Management

Infrastructure Protection

Judicial Bodies

Justice Bodies

Enforcement Support

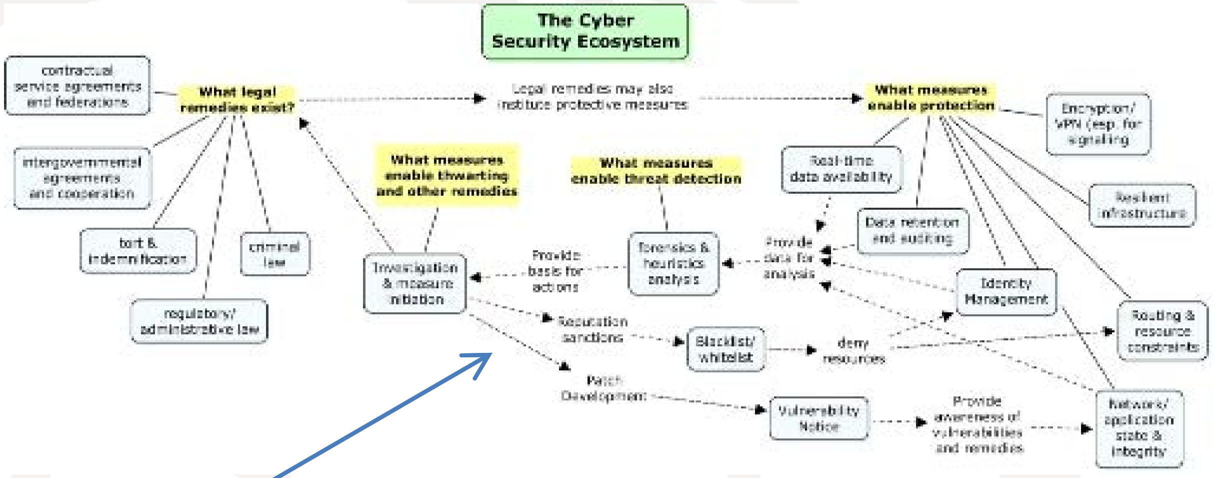
Security Bodies

Trusted Third Parties

This is a Global Problem

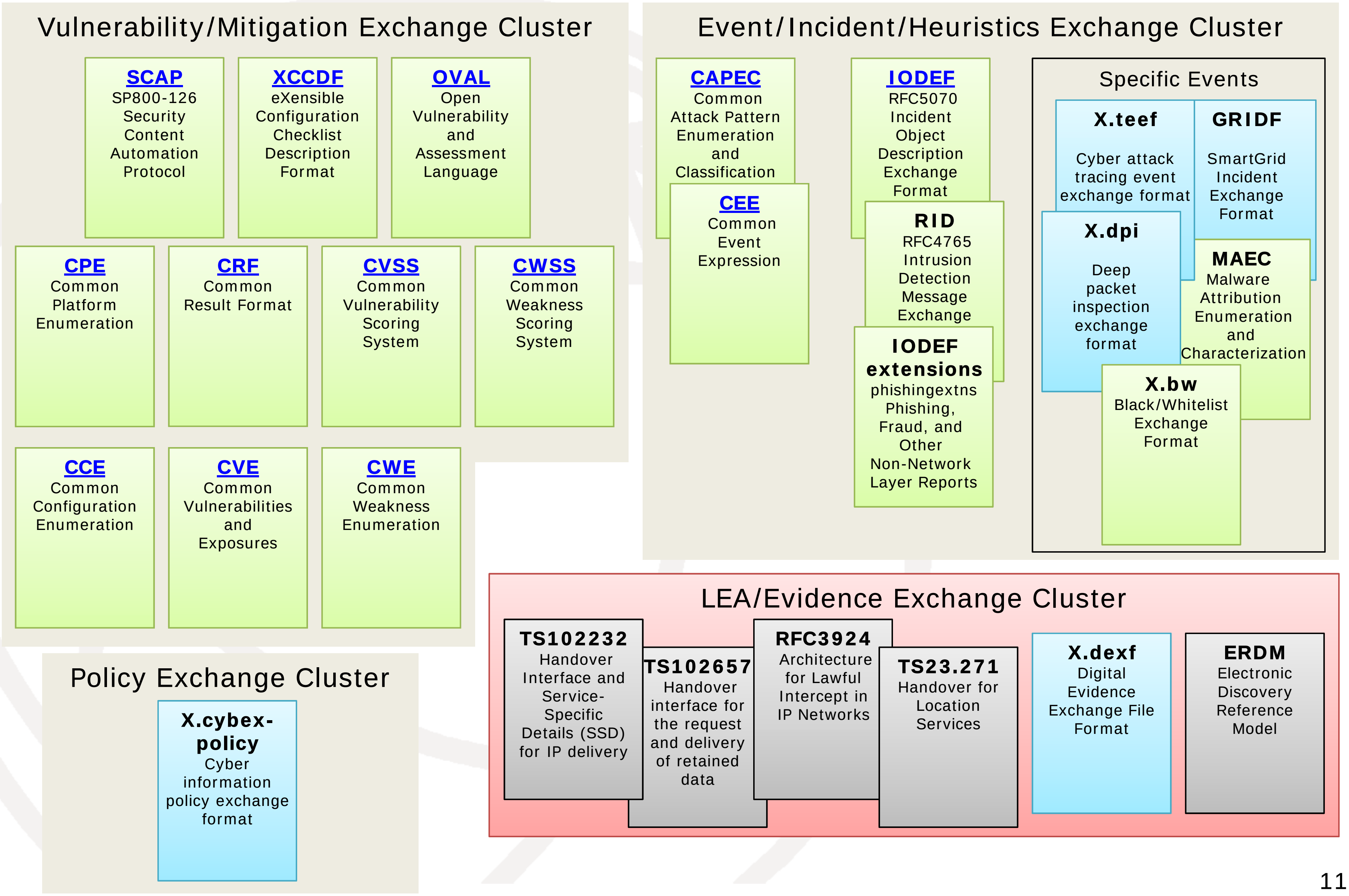
- Every nation is facing the same challenges
  - Collectively made global cyber security solutions, including facilitating capabilities for National CERTs, a priority at Nov 2008 ITU-T quadrennial meeting
  - Gave rise in 2009 to
    - A Cyber security Information Exchange (CYBEX) standards initiative in ITU-T largely based on newly developed government-industry solutions
    - Steps to expand Common Criteria
- Individual nations are taking steps
  - Mandating or incenting (with tort indemnification) infrastructure-based Identity Management and cyber security capabilities
  - Creating national CERTS

CYBEX starts the global focus


The Cyber Security Ecosystem
contractual service agreements and federations
What legal remedies exist?
Legal remedies may also institute protective measures
What measures enable protection
Encryption/ VPN (esp. for signaling
intergovernmental agreements and cooperation
What measures enable thwarting and other remedies
What measures enable threat detection
Real-time data availability
Resilient infrastructure
Data retention and auditing
tort & indemnification
criminal law
Investigation & measure initiation
Provide basis for actions
forensics & heuristics analysis
Provide data for analysis
Identity Management
Routing & resource constraints
regulatory/ administrative law
Reputation sanctions
Blacklist/ whitelist
deny resources
Patch Development
Vulnerability Notice
Provide awareness of vulnerabilities and remedies
Network/ application state & integrity

- CYBEX enables these capabilities by
  - ➢ Structuring the information
  - ➢ Coherent, trusted identification and discovery of the parties, information, and policies
  - ➢ Trusted exchange protocols
- CYBEX does not deal with how these capabilities get into place

Structured Information



Vulnerability/Mitigation Exchange Cluster

SCAP SP800-126 Security Content Automation Protocol

XCCDF eXensible Configuration Checklist Description Format

OVAL Open Vulnerability and Assessment Language

CPE Common Platform Enumeration

CRF Common Result Format

CVSS Common Vulnerability Scoring System

CWSS Common Weakness Scoring System

CCE Common Configuration Enumeration

CVE Common Vulnerabilities and Exposures

CWE Common Weakness Enumeration

Event/Incident/Heuristics Exchange Cluster

CAPEC Common Attack Pattern Enumeration and Classification

CEE Common Event Expression

IODEF RFC5070 Incident Object Description Exchange Format

RID RFC4765 Intrusion Detection Message Exchange

IODEF extensions phishingextns Phishing, Fraud, and Other Non-Network Layer Reports

Specific Events

X.teef Cyber attack tracing event exchange format

GRIDF SmartGrid Incident Exchange Format

X.dpi Deep packet inspection exchange format

MAEC Malware Attribution Enumeration and Characterization

X.bw Black/Whitelist Exchange Format

Policy Exchange Cluster

X.cybex-policy Cyber information policy exchange format

LEA/Evidence Exchange Cluster

TS102232 Handover Interface and Service-Specific Details (SSD) for IP delivery

TS102657 Handover interface for the request and delivery of retained data

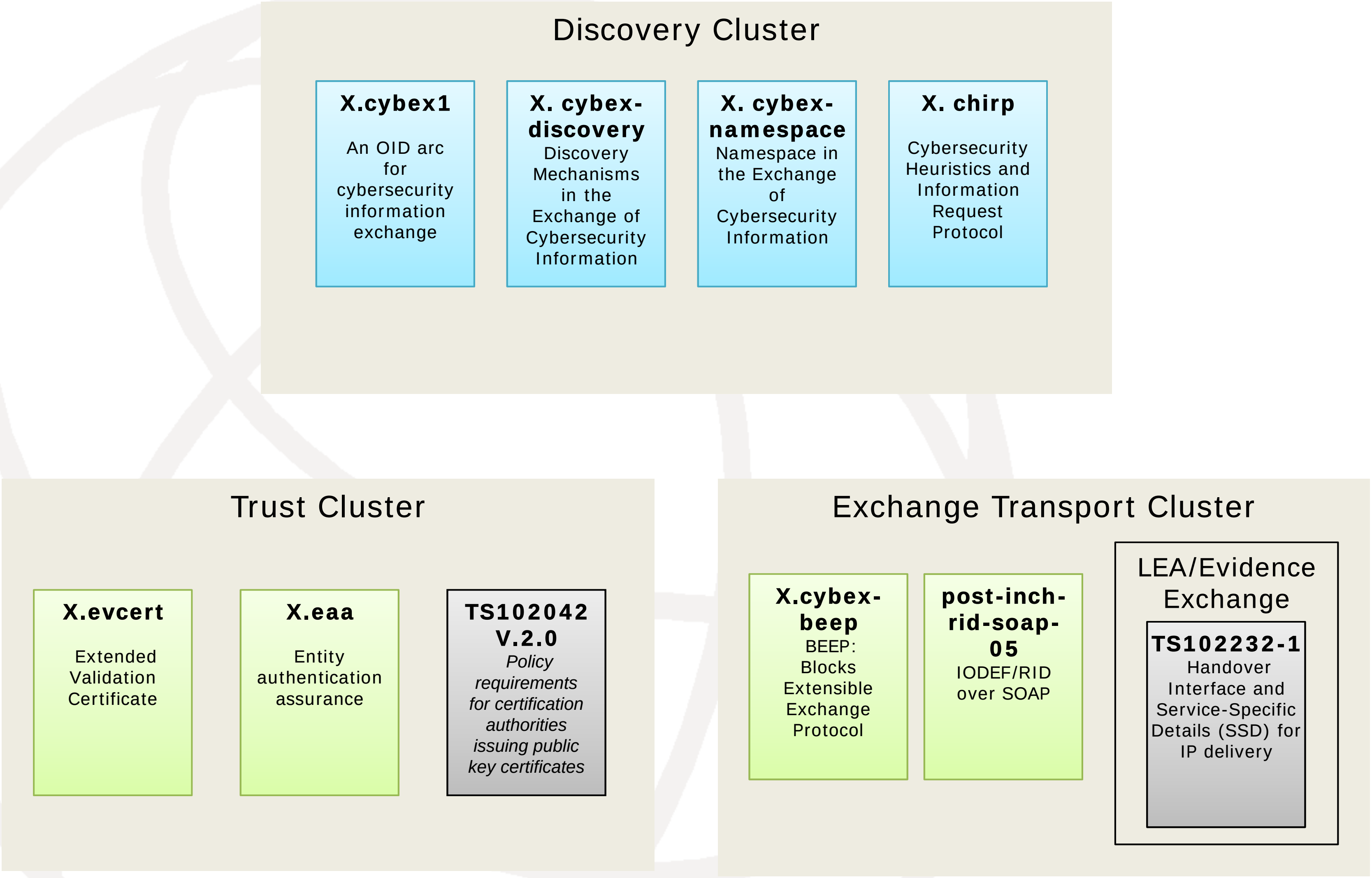
RFC3924 Architecture for Lawful Intercept in IP Networks

TS23.271 Handover for Location Services

X.dexf Digital Evidence Exchange File Format

ERDM Electronic Discovery Reference Model

Discovery and Trusted Exchange



Discovery Cluster

X.cybex1
An OID arc for cybersecurity information exchange

X. cybex-discovery
Discovery Mechanisms in the Exchange of Cybersecurity Information

X. cybex-namespace
Namespace in the Exchange of Cybersecurity Information

X. chirp
Cybersecurity Heuristics and Information Request Protocol

Trust Cluster

X.evcert
Extended Validation Certificate

X.eaa
Entity authentication assurance

TS102042 V.2.0
Policy requirements for certification authorities issuing public key certificates

Exchange Transport Cluster

X.cybex-beep
BEEP: Blocks Extensible Exchange Protocol

post-inch-rid-soap-05
IODEF/RID over SOAP

LEA/Evidence Exchange

TS102232-1
Handover Interface and Service-Specific Details (SSD) for IP delivery

The path forward

- ❑ Cyber security essentials
  - – The Commission
    - Mandates infrastructure and operational capabilities based on NSA requirements coordinated among relevant agencies
    - Indemnifies compliant providers and vendors
    - Implements strong identity management/attribution for providers and network identifiers
  - – Industry
    - Develops and implements standards based solutions
    - Meets compliance testing obligations
  - – Cooperate and act globally
- ❑ Remaining cyber security landmines
  - – Electrical systems/smart grids
  - – Network cloud infrastructures/services
  - – eHealth